I CLAIM:

1. A personal authentication device (PAD) comprising:

at least one storage medium storing at least one CA public key, each public key associated with a certificate authority (CA);

one or more input means for receiving one or more digital certificates;

a processing component for

authenticating the one or more received digital certificates using the at least one stored CA public key, and

generating at least one service key based on the one or more authenticated digital certificates; and

an output means for outputting at least one service key.

2. The personal authentication device (PAD) of claim 1, wherein the one or more digital certificates comprise at least one ticket-generation certificate indicating at least one service key generating program.

3. The personal authentication device (PAD) of claim 2, wherein the processing component comprises at least one component for

authenticating the at least one received ticket-generation certificate using the at least one stored CA public key; and

if one or more ticket-generation certificates are authenticated, generating the at least one service key based on the at least one authenticated service key generating program, wherein the at least one service key may be used by a user to obtain access to at least one service.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

4. The personal authentication device (PAD) of claim 2, wherein the one or more digital certificates comprises:

a user-identification certificate comprising information uniquely associated with a user;

and wherein the processing component comprises at least one component for

authenticating the received user-identification certificate using the at least one stored CA public key; and

if the user-identification certificate is authenticated, authenticating the user based on the authenticated user-identification certificate.

5. The personal authentication device (PAD) of claim 4, wherein the one or more digital certificates comprises:

at least one user-qualification certificate indicating at least one service and one or more users who may access the at least one service;

and wherein the processing component comprises at least one component for

authenticating the at least one received user-qualification certificate based on the at least one CA public key, if the user is authenticated; and

if the at least one user-qualification certificate is authenticated, determining at least one service that the authenticated user may have access to based on the at least one authenticated user-qualification certificate.

6. The personal authentication device (PAD) of claim 1, wherein the at least one service key comprises at least one cookie.

7. The personal authentication device (PAD) of claim 6, wherein the processing component comprises at least one component for:

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

generating a one-time key and storing it in PAD;

based on the one-time key, generating the at least one cookie and sending the generated cookie to the user;

receiving the previously generated the at least one cookie, and validating the received cookie using the stored one-time key; and

if the received cookie is successfully validated, invalidating the one-time key used in the cookie validation, generating a new one-time key and storing it in PAD, and based on the new one-time key, generating a new cookie and sending the new cookie to the user.

8. The personal authentication device (PAD) of claim 6, wherein the content in the one or more cookies comprises usage counts indicating the number of times one or more users have used one or more services.

9. The personal authentication device (PAD) of claim 5, wherein the one or more input means further receives one or more certificates comprising information for granting the user access to at least one additional service based on the at least one service.

10. The personal authentication device (PAD) of claim 1, wherein the at least one storage medium comprises at least one component for storing a PAD private key associated with the PAD.

11. The personal authentication device (PAD) of claim 10, wherein the one or more input means comprises at least one component for receiving a PAD authentication request; the processing component comprises at least one component for responding to the PAD authentication request using the stored PAD

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

private key; and the output means comprises at least one component for outputting responses to the PAD authentication request.

12. The personal authentication device (PAD) of claim 10, wherein the processing component comprises at least one component for signing the at least one service key using the stored PAD private key.

13. The personal authentication device (PAD) of claim 10, the processing component comprises at least one component for decrypting contents on the one or more received digital certificates using the stored PAD private key, wherein the contents are encrypted with the corresponding PAD public key.

14. The personal authentication device (PAD) of claim 5, wherein the one or more digital certificates comprise at least one ticket-generation certificate indicating at least one service key generating program corresponding to the at least one service; and wherein the processing component comprises at least one component for

authenticating the at least one ticket-generation certificate using the at least one stored CA public key; and

if one or more ticket-generation certificates are authenticated, generating the at least one service key based on the at least one authenticated service key generating program, wherein the at least one service key may be used by a user to obtain access to at least one service.

15. The personal authentication device (PAD) of claim 4, wherein the one or more input means further receives one or more user credentials, and the processing component comprises at least one component for

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

authenticating the user based on the authenticated user-identification certificate and the one or more received user credentials.

16. The personal authentication device (PAD) of claim 15, wherein the one or more user credentials comprise one or more user private keys.

17. The personal authentication device (PAD) of claim 15, wherein the one or more user credentials comprise a personal identification number (PIN) associated with the user, or information computed from the PIN.

18. The personal authentication device (PAD) of claim 15, wherein the one or more user credentials comprise biometric information associated with the user.

19. The personal authentication device (PAD) of claim 15, further comprising:

means for disabling the PAD if one or more attempts to authenticate the user based on the authenticated user-identification certificate and the one or more user credentials ends in failure.

20. The personal authentication device (PAD) of claim 1, wherein the one or more digital certificates comprises:

an operations certificate comprising information for controlling the operations of the PAD for a current session.

21. The personal authentication device (PAD) of claim 20, wherein the information for controlling the operations of the PAD for a current session comprises one or more of the following: information governing input and output of the PAD, challenge and response protocols for user and PAD authentication, secure protocols for receiving and outputting data, and protocols for PAD management purposes.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

22. The personal authentication device (PAD) of claim 20, wherein the information for controlling the operations of the PAD for a current session comprises information governing linking of one or more received certificates, and wherein the processing component comprises at least one component for linking of one or more received certificates based on one or more certificates comprising information for granting the user access to at least one additional service based on the at least one service.

23. The personal authentication device (PAD) of claim 1, wherein the one or more input means receive one or more signature-verification certificates forming a signature-verification chain, wherein each signature-verification certificate in the signature-verification chain is signed with the private key of an entity whose public key is certified by the preceding signature-verification certificate and wherein the first signature-verification certificate in the signature-verification chain is signed by at least one stored CA public key; and wherein the processing component comprises at least one component for authenticating the one or more received digital certificates based on the last signature-verification certificate in the signature-verification chain.

24. The personal authentication device (PAD) of claim 1, wherein the PAD is tamper-resistant.

25. The personal authentication device (PAD) of claim 10, wherein the CA public keys and the PAD private key are written into the PAD only once.

26. The personal authentication device (PAD) of claim 10, further comprising:

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

a protection mechanism that erases the PAD private key from the at least one storage medium when there are unauthorized attempts in reading or modifying the PAD private key.

27. The personal authentication device (PAD) of claim 1, wherein at least one of the one or more input means is a reading device capable of receiving at least one of the one or more digital certificates and user credentials from a storage medium or network interface.

28. The personal authentication device (PAD) of claim 1, further comprising a clock for determining a current date and time.

29. The personal authentication device (PAD) of claim 1, further comprising one or more timers for determining time that has elapsed since a timer was reset.

30. The personal authentication device (PAD) of claim 1, further comprising one or more counters for determining a number of times an event has occurred since a counter was reset.

31. The personal authentication device (PAD) of claim 1, wherein the one or more digital certificates further comprise information which may reset clock, timers and counters of the PAD.

32. The personal authentication device (PAD) of claim 1, wherein the one or more digital certificates comprise a content decryption key and content rights that the PAD will check before outputting the content decryption key as a service key.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

33. The personal authentication device (PAD) of claim 32, wherein the content rights comprise limits on at least one of the following: content expiration time, content usage period, content usage count.

34. The personal authentication device (PAD) of claim 28, wherein the processing component comprises at least one component for determining if the current date and time is within the validity period of the one or more received digital certificates.

35. The personal authentication device (PAD) of claim 28, wherein the processing component comprises at least one component for generating timestamps to be included in service keys that PAD 100 generates.

36. The personal authentication device (PAD) of claim 1, further comprising a write-once serial number.

37. The personal authentication device (PAD) of claim 36, wherein the processing component comprises at least one component for generating the at least one service key based on the serial number.

38. An authentication method comprising:

storing on a personal authentication device (PAD) at least one CA public key, each public key associated with a certificate authority (CA);

receiving one or more digital certificates;

authenticating the one or more received digital certificates using the at least one stored CA public key;

generating at least one service key based on the one or more authenticated digital certificates; and

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

outputting the at least one service key.

39. The method of claim 38, further comprising:

receiving at least one ticket-generation certificate indicating at least one service key generating program.

40. The method of claim 39, further comprising:

authenticating the at least one received ticket-generation certificate using the at least one CA public key; and

if the at least one ticket-generation certificate is authenticated, generating at least one service key based on the at least one service key generating program, wherein the at least one service key may be used by a user to obtain access to at least one service.

41. The method of claim 38, further comprising:

receiving a user-identification certificate comprising information uniquely associated with a user;

authenticating the received user-identification certificate based on the at least one CA public key; and

if the user-identification certificate is authenticated, authenticating the user based on the authenticated user-identification certificate.

42. The method of claim 41, further comprising:

receiving at least one user-qualification certificates indicating at least one service and one or more users who may access the at least one service;

authenticating the at least one received user-qualification certificate based on the at least one CA public key; and

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

if the at least one user-qualification certificate is authenticated, determining at least one service that the authenticated user may have access to based on the at least one authenticated user-qualification certificate.

43. The method of claim 38, wherein the at least one service key comprises at least one cookie.

44. The method of claim 38, further comprising:

generating a one-time key and storing it on the PAD;

based on the one-time key, generating the at least one cookie and sending the generated cookie to the user;

receiving the previously generated the at least one cookie, and validating the received cookie using the stored one-time key; and

if the received cookie is successfully validated, invalidating the one-time key used in the cookie validation, generating a new one-time key and store it on the PAD, and based on the new one-time key, generating a new cookie and sending the new cookie to the user.

45. The method of claim 44, wherein the content in the one or more cookies comprises usage counts indicating the number of times one or more users have used one or more services.

46. The method of claim 38, further comprising:

storing on the personal authentication device (PAD) a PAD private key associated with the PAD.

47. The method of claim 46, further comprising:

receiving a PAD authentication request;

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

responding to the PAD authentication request using the stored PAD private key; and

outputting the response to the PAD authentication request.

48. The method of claim 46, further comprising:

signing the at least one service key using the stored PAD private key.

49. The method of claim 46, further comprising:

decrypting contents on the one or more received digital certificates using the stored PAD private key, wherein the contents are encrypted with the corresponding PAD public key.

50. The method of claim 42, further comprising:

if the authenticated user is determined to have access to the services, authenticating the at least one ticket-generation certificate using the at least one CA public key; and

if the at least one ticket-generation certificate is authenticated, generating at least one service key based on the at least one service key generating program, wherein the at least one service key may be used by a user to obtain access to at least one service.

51. The method of claim 42, further comprising:

granting the user access to at least one additional service based on the at least one service and received digital certificate information.

52. The method of claim 41, further comprising:

receiving one or more received user credentials; and

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

authenticating the user based on the authenticated user-identification certificate and the one or more user credentials.

53. The method of claim 52, wherein the user credentials comprise one or more user private keys.

54. The method of claim 52, wherein the user credentials comprise a personal identification number (PIN) associated with the user, or information computed from the PIN.

55. The method of claim 52, wherein the user credentials comprise biometric information associated with the user.

56. The method of claim 52, further comprising:

disabling the PAD if one or more attempts to authenticate the user based on the authenticated user-identification certificate and the one or more user credentials ends in failure.

57. The method of claim 38, further comprising:

receiving an operations certificate comprising information for controlling the operations of the PAD for a current session.

58. The method of claim 57, wherein the information for controlling the operations of the PAD for a current session comprises one or more of the following: information governing input and output of the PAD, challenge and response protocols for user and PAD authentication, secure protocols for receiving and outputting data, and protocols for PAD management purposes.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

59. The method of claim 57, wherein the information for controlling the operations of the PAD for a current session comprises information governing linking of one or more received certificates, and wherein the method further comprises:

linking one or more received certificates based on one or more certificates comprising information for granting the user access to at least one additional service based on the at least one service.

60. The method of claim 38, further comprising:

receiving one or more signature-verification certificates forming a signature-verification chain, wherein each signature-verification certificate in the signature-verification chain is signed with the private key of an entity whose public key is certified by the preceding signature-verification certificate and wherein the first signature-verification certificate in the signature-verification chain is signed by at least one stored CA public key; and wherein the processing component comprises at least one component for authenticating the one or more received digital certificates based on the last signature-verification certificate in the signature-verification chain.

61. The method of claim 46, further comprising:

erasing the PAD private key when one or more unauthorized attempts to read or modify the PAD private key are detected.

62. The method of claim 38, wherein at least one of the one or more digital certificates is received from a storage medium or network interface.

63. The method of claim 38, further comprising determining a current date and time.

64. The method of claim 63, further comprising:

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

determining if the current date and time is within the validity period of the one or more received digital certificates.

65. The method of claim 38, further comprising determining elapsed time since a prior event.

66. The method of claim 38, further comprising determining the number of times an event has occurred since a prior event.

67. The method of claim 38, further comprising:

receiving one or more digital certificates which contain information for resetting current date and time, elapsed time, and a number of times an event has occurred.

68. The method of claim 67, further comprising:

resetting clock, timers or counters of the PAD based on information in the one or more digital certificates.

69. The method of claim 38, further comprising:

receiving one or more digital certificates which provide a content decryption key and content rights; and

checking the content rights before outputting the content decryption key as a service key.

70. The method of claim 69, wherein the content rights comprise limits on at least one of the following: content expiration time, content usage period, content usage count.

71. The method of claim 63, further comprising:

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

generating timestamps based on the current date and time, the timestamps to be included in service keys that the PAD generates.

72. The method of claim 38, further comprising:

generating the at least one service key based on a write-once serial number.

73. The method of claim 72, further comprising:

including the serial number in the at least one service key.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com